James R. Killian, Jr. Faculty Achievement Award 2010-11
Citation for *Ronald Rivest*

The Killian Award Committee is delighted to announce that the winner of the 2010-2011 James R. Killian Jr. Faculty Achievement Award is Professor Ronald Rivest, the Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science.

Professor Rivest is recognized for extraordinary contributions in computer science. He is one of the founding fathers of modern cryptography, especially of public key cryptography and digital signature methods. The basic concept of a public key system, articulated decades before the World Wide Web, allows any user to register a public key and retain a private key. By utilizing mathematical functions that are easy to compute but difficult to invert, messages can be encrypted and sent over a public channel with digital signatures attached, but only the intended recipient has the information to decrypt the message. It was the work of Professor Rivest and his colleagues Leonard Adelman and Adi Shamir that led to the design of a public key system, now known universally as the RSA system after its inventors, that was robust to sophisticated attack. It is also the first known algorithm that supports both encryption and digital signing to authenticate the sender. While the code for RSA is deceptively simple, it has not been broken in the more than four decades since its invention.

At the time of publication of their fundamental papers, the practicality of any cryptosystem seemed remote and the RSA system was perceived as an important theoretical contribution with limited practical implications. Now it is a widely used standard, playing a critical role in the widespread use and success of the internet and internet-based commerce. The RSA code is a wonderful example of elegant and abstract theory eventually having immense practical impact.

Prof. Rivest's contributions to the impact of RSA move from deep fundamental inquiry to practical development and technology transfer as the active founder of two of the most successful Internet security companies. As noted in one of the nomination letters, "Ron has the cultural background required to perceive the larger influence of scientific innovation, and the moral strength, energy and eloquence necessary to drive it towards its proper use."

While Prof. Rivest is most widely known for his work in cryptography and security, he has made important contributions in many other areas of computer science including computer-aided design of integrated circuits, data structures, and computer algorithms. He is also acknowledged as an early contributor to the field of machine learning.

Throughout his career, Professor Rivest has received numerous awards and honors for his scholarship and contributions. Particularly notable are the Turing Award and the Marconi Prize. The Turing Award is generally regarded as the most prestigious award in computer science. The Marconi Prize, established in 1975 by the Marconi Society, "annually

recognizes a living scientist whose work in the field of communications and information technology advances the social, economic and cultural improvement of all humanity."

Professor Rivest is also a dedicated and legendary teacher, mentor and educator. His textbook *Introduction to Algorithms*, co-authored with Prof. Cormen and Prof. Leiserson, grew out of the undergraduate and graduate courses on computer algorithms. This text reflects Prof. Rivest's dedication to teaching and to finding elegant ways of explaining complex ideas. It is currently the second most cited reference in all of computer science. As a mentor he has been an inspiring role model for his students and colleagues. His wisdom and insights are continually sought by students and colleagues and as commented in the nomination letters, he is always extraordinarily generous with his time. Among his many contributions within MIT have been his guidance, wisdom and leadership as co-chair of the committee for the re-organization of the Artificial Intelligence Laboratory and the Laboratory for Computer Science. The new combined laboratory, CSAIL, is now the largest laboratory on the MIT campus.

It is with great pleasure that we announce the choice of Professor Rivest as the recipient of the 2010-2011 James R. Killian Jr. Faculty Achievement Award for his outstanding accomplishments as a scholar, teacher, mentor, and leader internationally and within our community.